The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/20/2017

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been identified in Mozilla Firefox and Firefox Extended Support Release (ESR), which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There is no evidence of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 53
- Firefox ESR versions prior to 45.9 and 52.1

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Mozilla has confirmed the following vulnerabilities in Firefox and Firefox Extended Support Release (ESR).

- A use-after-free vulnerability in SMIL animation functions occurs when pointers to animation elements in an array are dropped from the animation controller while still in use. (CVE-2017-5433).

- A use-after-free vulnerability occurs during transaction processing in the editor during design mode interactions. (CVE-2017-5435)
- An out-of-bounds write in the Graphite 2 library triggered with a maliciously crafted Graphite font. (CVE-2017-5436)
- An out-of-bounds write during Base64 decoding operation in the Network Security Services (NSS) library due to insufficient memory being allocated to the buffer. (CVE-2017-5431, CVE-2017-5461)
- A buffer overflow in WebGL triggerable by web content. (CVE-2017-5459)
- If a page is loaded from an original site through a hyperlink and contains a redirect to a data:text/html URL, triggering a reload will run the reloaded data:text/html page with its origin set incorrectly. This allows for a cross-site scripting (XSS) attack. (CVE-2017-5466)
- A use-after-free vulnerability occurs when redirecting focus handling. (CVE-2017-5434)
- A use-after-free vulnerability occurs during certain text input selection. (CVE-2017-5432)
- A use-after-free vulnerability in frame selection triggered by a combination of malicious script content and key presses by a user. (CVE-2017-5460)
- A use-after-free vulnerability during XSLT processing due to the result handler being held by a freed handler during handling. (CVE-2017-5438)
- A use-after-free vulnerability during XSLT processing due to poor handling of template parameters. (CVE-2017-5439)
- A use-after-free vulnerability during XSLT processing due to a failure to propagate error conditions during matching while evaluating context, leading to objects being used when they no longer exist. (CVE-2017-5440)
- A use-after-free vulnerability when holding a selection during scroll events. (CVE-2017-5441)
- A use-after-free vulnerability during changes in style when manipulating DOM elements. (CVE-2017-5442)
- During DOM manipulations of the accessibility tree through script, the DOM tree can become out of sync with the accessibility tree. (CVE-2017-5464)
- An out-of-bounds write vulnerability while decoding improperly formed BinHex format archives. (CVE-2017-5443)
- A buffer overflow vulnerability while parsing application/http-index-format format content when the header contains improperly formatted data. (CVE-2017-5444)
- An out-of-bounds read when an HTTP/2 connection to a servers sends DATA frames with incorrect data content. (CVE-2017-5446)
- An out-of-bounds read during the processing of glyph widths during text layout. (CVE-2017-5447)
- An out-of-bounds read while processing SVG content in ConvolvePixel. (CVE-2017-5465)
- An out-of-bounds write in ClearKeyDecryptor while decrypting some Clearkey-encrypted media content. The ClearKeyDecryptor code runs within the Gecko Media Plugin (GMP) sandbox. (CVE-2017-5448)
- Three vulnerabilities were reported in the Libevent library that allow for out-of-bounds reads and denial of service attacks: CVE-2016-10195, CVE-2016-10196, and CVE-2016-10197. (CVE-2017-5437)
- A mechanism to bypass file system access protections in the sandbox to use the file picker to access different files than those selected in the file picker through the use of relative paths. (CVE-2017-5454)
- The internal feed reader APIs that crossed the sandbox barrier allowed for a sandbox escape and escalation of privilege if combined with another vulnerability that resulted in remote code execution inside the sandboxed process. (CVE-2017-5455)

- A mechanism to bypass file system access protections in the sandbox using the file system request constructor through an IPC message. (CVE-2017-5456)
- Fixed potential buffer overflows in generated Firefox code due to CVE-2016-6354 issue in Flex. (CVE-2017-5469)
- A vulnerability while parsing application/http-index-format format content where uninitialized values are used to create an array. (CVE-2017-5445)
- A possibly exploitable crash triggered during layout and manipulation of bidirectional unicode text in concert with CSS animations. (CVE-2017-5449)
- A mechanism to spoof the Firefox for Android addressbar using a javascript: URI. (CVE-2017-5450)
- A mechanism to spoof the addressbar through the user interaction on the addressbar and the onblur event. (CVE-2017-5451)
- A flaw in DRBG number generation within the Network Security Services (NSS) library where the internal state V does not correctly carry bits over. (CVE-2017-5462)
- Android intents can be used to launch Firefox for Android in reader mode with a user specified URL. (CVE-2017-5463)
- A potential memory corruption and crash when using Skia content when drawing content outside of the bounds of a clipping region. (CVE-2017-5467)
- Malicious sites can display a spoofed addressbar on a page when the existing location bar on the new page is scrolled out of view if an HTML editable page element is user selected. (CVE-2017-5452)
- A mechanism to inject static HTML into the RSS reader preview page due to a failure to escape characters sent as URL parameters for a feed's TITLE element. (CVE-2017-5453)
- When a javascript: URL is drag and dropped by a user into the addressbar, the URL will be processed and executed. (CVE-2017-5458)
- An issue with incorrect ownership model of privateBrowsing information exposed through developer tools. (CVE-2017-5468)
- Memory safety bugs present in Firefox 52, Firefox ESR 45.8, and Firefox ESR 52 showed evidence of memory corruption and it is presumed that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2017-5429, CVE-2017-5430)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2017-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-12/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5429
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5430
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5431
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5432
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5433
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5434
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5435
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5436
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5437
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5438
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5439
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5440
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5441
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5442
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5443
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5444
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5445
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5446
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5447
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5448
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5449
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5450
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5451
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5452
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5453
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5454
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5455
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5456
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5458
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5459
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5460
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5461
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5462
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5463
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5464
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5465
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5466
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5467
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5468
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5469